BakerHostetler

Baker&Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Theodore J. Kobus III
direct dial: 212.271.1504
tkobus@bakerlaw.com

March 17, 2015

VIA OVERNIGHT DELIVERY

Office of the Attorney General
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut St.
Des Moines, IA 50319

Re: Incident Notification

Dear Sir or Madam:

Our client, Premera Blue Cross, including its affiliates Academe, Inc. (formerly known as LifeWise Health Plan of Arizona, Inc.), Connexion Insurance Solutions, Inc., LifeWise Health Plan of Washington, LifeWise Health Plan of Oregon, Inc., LifeWise Assurance Company, and Vivacity, Inc. (collectively ("Premera")), on January 29, 2015, discovered that cyber-attackers had executed a sophisticated attack to gain unauthorized access to its Information Technology (IT) systems. Further investigation revealed that the initial attack occurred on May 5, 2014. Premera worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct its investigation and to remove the infection created by the attack on its IT systems. Premera notified the FBI and continues to work closely with the agency on its investigation.

Premera's investigation has determined that the attackers may have possibly gained unauthorized access to members' and other individuals' personal information, including names, addresses, telephone numbers, dates of birth, Social Security numbers, member identification numbers, bank account information, email addresses if provided, and claims information, including clinical information. Premera acquires this information in its capacity as a health plan, as an administrator for self-funded accounts, as a service provider, or as a participant in the national BlueCard program.[1] In all cases and without waiving any objection to personal

[1] Premera participates in the national BlueCard program, which allows a member in one Blue Cross Blue Shield (BCBS) plan to get high-quality affordable health care they need wherever they are form providers that participate in a different BCBS plan's network. If an individual received healthcare in Washington or Alaska (Premera's home

jurisdiction or ERISA-preemption, this notice is intended to satisfy obligations for Premera, its self-funded accounts and customers, Blue Cross Blue Shield (BCBS) plans and BCBS plans' self-funded accounts to notify your office about this incident.

The investigation has not determined that any such data was removed from Premera's systems. We also have no evidence to date that such data has been used inappropriately.

Although we know of no reports of identity theft or other fraud related to this incident, Premera is beginning to notify individuals affected by the incident on March 17, 2015. Premera is offering affected individuals two years of complimentary credit monitoring and identity theft protection services through Experian. Premera also is providing call center support for those affected. In addition, Premera is recommending that members regularly review their explanation of benefits statements for suspicious activity. Should any member identify a medical service listed on an explanation of benefits statement that was not received, the member should immediately contact Premera.

Premera is notifying Iowa residents pursuant to Iowa statute in substantially the same form as the letters attached hereto.[2] As a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Premera is required to maintain procedures for responding to a breach of security, and notification to Iowa residents who are members is being provided in compliance with these procedures. *See* IOWA CODE ANN. § 715C.2(7)(a); *see also* 45 C.F.R. §§ 160.103 and 164.400 *et seq.*

Notification is being provided in the most expeditious manner possible and without unreasonable delay pursuant to the investigation described above, which was necessary to determine the scope of the incident; restore the reasonable integrity, security, and confidentiality of the data; and identify the individuals potentially affected. *See* IOWA CODE ANN. § 715C.2(1).

In addition to cleansing its IT systems of the issues raised by this cyberattack and to help prevent something like this from happening in the future, Premera has taken actions to strengthen and enhance the security of its IT systems moving forward.

---

states), health care providers in Washington and Alaska may have shared information with Premera in order to process claims.

[2] This report is not, and does not constitute, a waiver of personal jurisdiction.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Theodore J. Kobus III

Enclosures

[Premera Letterhead]

March [X], 2015

Member First and Last Name
Street Address
City, State Zip Code

Dear Member First and Last Name:

I am writing to inform you that Premera Blue Cross ("Premera") was the target of a sophisticated cyberattack, and that some of your personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are coordinating with their own investigation into this attack.

We at Premera take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect you and your information moving forward.

What happened?
On January 29, 2015, we discovered that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on May 5, 2014. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remove the infection created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your information, which could include your name, address, telephone number, date of birth, Social Security number, member identification number, bank account information, email address if provided to us, and claims information, including clinical information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

What is Premera doing to protect you?
We recognize this issue can be frustrating and we are taking steps to protect you. We are providing protection and assistance to those affected by this cyberattack, including two years of free credit monitoring and identity theft protection services.

Specifically, we are providing you a **free, two-year membership in Experian's® ProtectMyID® Alert** to help detect possible misuse of your personal information and provide you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. Due to privacy laws, we are not able to enroll you directly. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your free, two-year membership, please see the additional information provided in this letter.**

We also recommend that you regularly review the Explanation of Benefits (EOB) statements Premera sends you. If you identify medical services listed on your EOB that you did not receive, please contact us immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your bank account or change your bank account number, please contact your bank.

What has Premera done to prevent this from happening in the future?
Along with steps we took to cleanse our IT system of issues raised by this cyberattack, Premera is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

Where can you get more information on this issue?
You have two options to obtain more information, online or via phone. You can visit http://www.premeraupdate.com for more information. Or, call 1-800-768-5817, Monday through Friday, 5:00 a.m. to 8:00 p.m. Pacific Time (closed on U.S. observed holidays). TTY/TDD users should call 1-877-283-6562.

I want you to know that protecting your information is incredibly important to us at Premera, as is helping you through this situation with the information and support you need.

Sincerely,

Jeffrey Roe
President & CEO

Activate ProtectMyID Now in Two Easy Steps

1. ENSURE **That You Enroll By: September 30, 2015** (You will not be able to enroll after this date.)
2. VISIT the **ProtectMyID Web Site: www.protectmyid.com/premera**

If you have questions related to the product being offered or need an alternative to enrolling online, please call 888-451-6558 and provide engagement #: **PC92585**

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report:** See what addresses, employers, public records and accounts are already associated with you.
- **Alerts for:**
  - **3-Bureau Credit Monitoring:** Alerts you of new accounts appearing on your Experian, Equifax® and TransUnion® credit reports.
  - **3-Bureau Active Fraud Surveillance:** Daily monitoring of 50 potential indicators of fraud appearing on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 888-451-6558.

INFORMATION ABOUT PREVENTING IDENTITY THEFT

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit

---

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 2002	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

[Premera Letterhead]

March [X], 2015

Parent or Guardian of Member First and Last Name
Street Address
City, State Zip Code

Dear Parent or Guardian of Member First and Last Name:

I am writing to inform you that Premera Blue Cross ("Premera") was the target of a sophisticated cyberattack, and that some of your child's personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are coordinating with their own investigation into this attack.

We at Premera take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect you and your child's information moving forward.

What happened?
On January 29, 2015, we discovered that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on May 5, 2014. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remove the infection created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your child's information, which could include your child's name, address, telephone number, date of birth, Social Security number, member identification number, bank account information, email address if provided to us, and claims information, including clinical information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

What is Premera doing to protect you?
We recognize this issue can be frustrating and we are taking steps to protect you and your child. We are providing protection and assistance to those affected by this cyberattack, including two years of free credit monitoring and identity theft protection services.

Specifically, we are offering you a **free two-year membership in Family Secure®** from Experian®. Family Secure monitors your Experian credit report to notify you of key changes. In addition, Family Secure will tell you if your minor has a credit report, a potential sign that his or her identity has been stolen. Family Secure is completely free and will not hurt your credit score. **For more information about Family Secure and instructions on how to activate the complimentary one-year membership, please see the additional information provided in this letter.**

We also recommend that you regularly review the Explanation of Benefits (EOB) statements Premera sends your child. If you identify medical services listed on your child's EOB that your child did not receive, please contact us immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your child's bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your child's bank account or change your child's bank account number, please contact your child's bank.

What has Premera done to prevent this from happening in the future?
Along with steps we took to cleanse our IT system of issues raised by this cyberattack, Premera is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

Where can you get more information on this issue?
You have two options to obtain more information, online or via phone. You can visit http://www.premeraupdate.com for more information. Or, call 1-800-768-5817, Monday through Friday, 5:00 a.m. to 8:00 p.m. Pacific Time (closed on U.S. observed holidays). TTY/TDD users should call 1-877-283-6562.

I want you to know that protecting your information is incredibly important to us at Premera, as is helping you through this situation with the information and support you need.

Sincerely,

Jeffrey Roe
President & CEO

To receive the complimentary Family Secure product, you as the parent or guardian of the minor must enroll at the web site below.

Activate Family Secure Now in Two Easy Steps

1. ENSURE **That You Enroll By: September 30, 2015** (Your activation will not work after this date.)
2. VISIT the **Family Secure Web Site to enroll: http://www.familysecure.com/premera**

If you have questions related to the product being offered or need an alternative to enrolling online, please call 888-451-6558 and provide engagement #: **PC92586**

What features does your 24-MONTH Family Secure membership include once activated?

Parent or Legal Guardian:

- Daily monitoring of your Experian credit report with email notification of key changes, as well as monthly "no-hit" reports
- 24/7 credit report access: Unlimited, on-demand Experian reports and scores
- Experian credit score illustrator to show monthly score trending and analysis

Children:

- Monthly monitoring to determine whether enrolled minors in your household have an Experian credit report
- Alerts of key changes to your children's Experian credit report

All Members:

- Identity Theft Resolution assistance: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies
- $2,000,000 Product Guarantee*

Once your enrollment in Family Secure is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about Family Secure, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 888-451-6558.

INFORMATION ABOUT PREVENTING IDENTITY THEFT

In addition, we recommend that you remain vigilant to the possibility of fraud and identity theft over the next 12 to 24 months by reviewing your child's account statements and immediately reporting any suspicious activity to us. You may also obtain a copy of your child's credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your child's credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You should periodically obtain credit reports from each of the nationwide credit reporting agencies and request that any fraudulent activity be deleted. Contact information for the three nationwide credit reporting agencies is as follows:

---

* The Family Secure Product Guarantee is not available for Individuals who are residents of the state of New York.

Equifax	Experian	TransUnion
PO Box 740241	PO Box 2002	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

If you believe you or your child is the victim of identity theft or have reason to believe your or your child's personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your or your child's records.

Deceased

[Premera Letterhead]

March [X], 2015

Estate of Member First and Last Name
Street Address
City, State Zip Code

Dear Estate of Member First and Last Name:

I am writing to inform you that Premera Blue Cross ("Premera") was the target of a sophisticated cyberattack, and that some of your family member's personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are coordinating with their own investigation into this attack.

We at Premera take this issue seriously and regret the concern it may cause. Our regret is compounded by the fact that we know you lost your family member, which may make this more difficult to receive. I'm writing to provide you information on the steps we are taking to protect your family member's information moving forward.

What happened?
On January 29, 2015, we discovered that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on May 5, 2014. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remove the infection created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your family member's information, which could include your family member's name, address, telephone number, date of birth, Social Security number, member identification number, bank account information, email address if provided to us, and claims information, including clinical information. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

What is Premera doing to protect your family member?
We recognize this issue can be frustrating and we wanted to assure you that we are diligently investigating the incident. However, if you still receive Explanation of Benefits (EOB) statements from Premera regarding your family member, we recommend that you review them. If you identify medical services listed on the EOB that your family member did not receive, please contact us immediately. We further recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your family member's bank, credit card and other financial statements for any unauthorized activity. If you would like to place an alert on your family member's bank account or change your family member's bank account number, please contact your family member's bank.

What has Premera done to prevent this from happening in the future?
Along with steps we took to cleanse our IT system of issues raised by this cyberattack, Premera is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

Where can you get more information on this issue?
You have two options to obtain more information, online or via phone. You can visit http://www.premeraupdate.com for more information. Or, call 1-800-768-5817, Monday through Friday, 5:00 a.m. to 8:00 p.m. Pacific Time (closed on U.S. observed holidays). TTY/TDD users should call 1-877-283-6562.

I want you to know that protecting your information is incredibly important to us at Premera, as is helping you through this situation with the information and support you need.

Sincerely,

Jeffrey Roe
President & CEO